UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with cellular telephone number (414) 779-3186, as more fully described in Attachment A.	)	Case No.22-1843M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 12/5/2022 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 11/21/2022 @ 1:02 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

1. Records and information associated with:

    - the cellular device assigned call number **(414) 779-3186** (referred to herein and in Attachment B as **"Target Cell Phone 1"** or "**TCP-1**"), that is in the custody or control of AT&T Mobility (referred to herein and in Attachment B as the "Service Provider" or "Provider"), a wireless communications service provider that is headquartered at 11760 U.S. Highway 1, Suite 600, North Palm Beach, FL 33408.

2. Target Cell Phone 1.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with **TCP-1** for the time period from February 1, 2021, to present:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

   vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);

   viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by **TCP-1**, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(B) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received).

b. Information associated with each communication to and from **TCP-1** for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which **TCP-1** or will connect at the beginning and end of each communication.

The Court has also issued an order(s) pursuant to 18 U.S.C. § 3123, dated today, for such information associated with **TCP-1**.

c. Information about the location of **TCP-1** for a period of **30 days**, during all times of day and night. "Information about the location of TCP-1" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of **TCP-1** on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), and 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) since February 2021.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with cellular telephone number (414) 779-3186, as more fully described in Attachment A.

Case No. 22-1843M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1347 and 1035; 42 U.S.C. Section 1320a-7b	Healthcare Fraud: False Statements Related to Healthcare: Illegal Kickbacks

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Jill Dring
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date 11/21/2022:

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jill A. Dring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number (414) 779-3186 ("**Target Cell Phone 1**" or "**TCP-1**"). **TCP-1** service provider is AT&T Mobility (the "Service Provider"), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, Suite 600, North Palm Beach, FL 33408. **TCP-1** associated with SAMONE THOMAS (DOB: 02/05/1990). **TCP-1** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application(s) by the United States of America for an order(s) pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from **TCP-1**.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March of 2013. As a Special Agent, I investigate civil and criminal matters related to health care fraud involving violations of the Health Care Fraud Statute, False Claims Act, Anti-Kickback Statute and Stark Law. Prior to investigating health care fraud matters, I investigated criminal and

national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of identification information, and other computer-based fraud. I have received training in computer technology, computer-based fraud and health care fraud.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Throughout this affidavit, reference will be made to case agents. Case agents are those federal and state law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact regarding this investigation. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) have been committed, are being committed, or will be committed by PRECIOUS CRUSE (DOB: 06/07/1993) and others known and unknown to the case agents. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses.

6. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On 9/28/21, members of the Medicaid Fraud Control & Elder Abuse Unit (MFCEAU), were assigned Department of Justice Investigation case number 2021-07738, involving a credible allegation of fraud referral from Department of Health Services (DHS) Office of the Inspector General (OIG) pertaining to Caring Through Love, a Prenatal Care Coordination (PNCC) agency owned by PRECIOUS CRUSE. A Prenatal Care Coordination (PNCC) agency is an agency that provides services to pregnant women who are at high risk for adverse pregnancy outcomes. PNCC services are reimbursed under Wisconsin Medicaid when provided in accordance with Wisconsin Medicaid's rules and regulations. Covered services related to PNCC services are listed in Wis. Admin. Code § DHS 107.34.

8. Per Wis. Admin. Code § DHS 107.34, PNCC agencies are required to have a Qualified Professional. Prior to services being performed for a Medicaid recipient by a PNCC, and the subsequent reimbursement by Wisconsin Medicaid, an initial assessment and care plan are required. The Qualified Professional reviews and signs the assessment.

9. The PNCC program requires providers to submit accurate and truthful claims for payments. It also requires a provider to only seek reimbursement for the actual amount of time spent assisting a member. And it prohibits providers from seeking reimbursement for non-covered services. Examples of non-covered services include personal comfort items such as radios and television sets. DHS 107.03(6). Additionally, DHS has explained that if a client is in need of something like diapers or wipes, a care coordinator should connect the client with an organization that can provide those items, rather than providing them. The PNCC program prohibits seeking reimbursement for noncovered services by charging for a covered service that was not actually provided.

10. On 9/28/21, MFCEAU accepted a credible allegation of fraud referral from DHS OIG. The allegations stated that Caring Through Love, LLC (CTL), offered illegal incentives to its members and/or prospective members to enroll in the program. Additionally, there are allegations that CTL, intentionally made false statements or representations of material facts on a claim to obtain payment for services provided without the supervision of a Qualified Professional.

11. According to records kept by DHS in the regular course of its official business, Vivian Mealing, RN, is listed as the Qualified Professional at CTL. Barbara Hayden, an OIG nurse consultant, contacted Vivian Mealing, and during a conversation that occurred on 4/1/21, Mealing informed Hayden that she has yet to perform any services for CTL.

12. DHS launched and completed an investigation prior to sending MFCEAU the credible allegation of fraud. DHS reviewed Facebook posts of Presh Hutchinson that appeared to offer monetary incentives to clients for Mother's Day. As substantiation for the allegation, DHS OIG provided a screenshot or screen capture of the Facebook post made by Presh Hutchinson. A screenshot or screen capture is a digital image that shows the content of a computer or digital display.

13. Case agents reviewed the screenshot provided by DHS OIG. The screenshot in question is a Facebook post from 05/27/2021, posted under the account of Presh Hutchinson. It reads, "Happy Mother's Day To All the Clients Enrolled With Caring Through Love LLC We Appreciate Yall, & I hope Yall Enjoy Your Gifts From Us & Your Day." A photograph and video are attached to the post. In the photo, and screen still from the video, there is $100 in $20 bills in a card.

14. Based on my training and experience, I know that Wisconsin Medicaid does not allow monetary incentives to potential or existing clients, and it is viewed as an illegal incentive,

or a kickback. The Wisconsin Medicaid Provider Agreement and Acknowledgement of Terms of Participation (WMPAATP), set forth by Wis. State § 49.045(2)(a)9, and Wis. Admin Code §DHS 105.01, state that a provider, in this case CRUSE and CTL understands and agrees that every time the provider signs and submits a claim, the provider certifies that the provider has not offered, paid, or received any illegal remuneration or any other thing of value in return for referring an individual to a person for the furnishing of any service or item, or for arranging for the furnishing of any service or item for which payment may be made in whole or in part under Medical Assistance in violation of 42 U.S.C. § 1320a-7b, Wis. Stat. § 946.91(3), or any other federal or state anti-kickback statutes. The WMPAATP was signed by CRUSE on 02/04/2021.

15. Case agents reviewed Wisconsin Medicaid records kept by DHS in the regular course of its official business and learned that CRUSE is the current and past owner of CTL. Case agents confirmed that CRUSE was the owner of CTL, at the times of the suspect posts.

16. In February 2022, I joined MECEAU's investigation of CTL.

17. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan interviewed Tia Imes, who was a registered client of CTL. CTL business records demonstrated that SAMONE THOMAS was Tia Imes' care coordinator. CTL billed $1,056 to Medicaid for PNCC services purportedly provided to Ms. Imes on 10 separate dates. Ms. Imes told investigators that she signed up for services with CTL at a "community baby shower" at which she received diapers, wipes, and a pack 'n play. Ms. Imes said that she was never thereafter contacted by anyone with CTL and received no services. The first day of service billed for Ms. Imes was August 6, 2021. Ms. Imes states that she was in the hospital recovering from the birth of her child that day and did not meet anyone from CTL that day.

18. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan, interviewed Tenisha Woulard. Woulard was a client of CTL. CTL billed $2,112 for services purportedly provided to Ms. Woulard on 22 separate occasions. She indicated during the interview that she received no services and only had one meeting with a representative from CTL. THOMAS was listed as Ms. Woulard's care coordinator.

19. On October 3, 2022, I, along with MECEAU investigator Rory O'Sullivan, interview three other women for whom CTL submitted billing claims to Medicaid for PNCC services purportedly provided by THOMAS. All the women indicated that they received no coordination services. Some indicated that they received outfits, diapers, and fireworks. We showed these clients billing records describing meetings and services purportedly provided. Each denied that the meetings occurred or that the services were provided. At least one woman interviewed denied knowing THOMAS.

20. On November 16, 2022, I, along with Rory O'Sullivan and AUSAs Julie Stewart and Kate Biebel, interviewed THOMAS. During the meeting, she produced her cellular phone, an Apple iPhone, and consulted it on several occasions to view photos and videos while responding to our questions. I know the phone number associated with THOMAS's iPhone is (414) 779-3186; I know this because AUSA Stewart called THOMAS on that number, which THOMAS previously provided, on the morning of November 16, 2022 to confirm the meeting. THOMAS stated she forgot and asked AUSA Stewart to text her the address of building where the meeting was to take place. AUSA Stewart sent a text message to that number with the information THOMAS had requested, and THOMAS soon thereafter arrived at the address AUSA Stewart had provided. After the meeting ended, I sent a text message to THOMAS at that number and she responded.

21. During the meeting, THOMAS indicated that the woman who denied knowing her was "her cousin." She also said that it was not true that she provided no services to these women.

22. THOMAS acknowledged during this meeting, however, that the billing records that contained her name and described services provided were not accurate or truthful. She said that the entries in those records were written or provided by CRUSE. Each entry on the forms showed to THOMAS stated that THOMAS met with a particular client for 2 hours. Many records included an entry for a 2-hour meeting multiple times in a month. THOMAS denied meeting with her clients for two hours at a time on that many occasions. She said she typically contacted her clients once per month. She said that she did not fill out the forms or submit those billings and that CRUSE was responsible for doing so.

23. THOMAS acknowledged that she did not know Ms. Imes and likely did not provide services to her.

24. THOMAS stated that she was not provided training on how to provide services to her clients or told what to do. She stated that many of her clients told her that they did not need any prenatal care coordination services. As a result, she tried to give them something else they might need by, for example, giving their children fireworks for the Fourth of July.

25. During the interview on November 16, 2022, THOMAS stated that she had communications with CRUSE over Facebook and via text. She thought she may have deleted the text messages, but believed she might still have the Facebook communications on her phone.

26. During the interview on November 16, 2022, THOMAS stated that she had used her phone to video-record a meeting in which CRUSE "did the billing" for the PNCC CTL. She stated that she attended such sessions on a monthly basis during her employment at CTL, which she indicated spanned from June 2021 to sometime in August 2021. THOMAS stated that she

filmed this meeting on August 6, 2021 during which CRUSE "did the billing" because she was not taking notes. She said that CRUSE explained how to fill out the billing sheets. THOMAS told investigators that CRUSE told her not to film it, but that she did anyway. THOMAS showed investigators portions of that video during the interview. During those protions, the screen showed an image of a billing record that included time spent and a description of a service provided. CRUSE could be heard on the video instructing the cooridnators not to change the sections that detailed the service provided and to only change the portion of the document that included the care coordinator's name and client's name. THOMAS explained that this was standard – that the billing forms all included essentially the same information for services provided and that CRUSE documented the time spent (almost always 2 hours), and that care coordinators were instructed to only fill in their names and their client names on these billing records.

27. THOMAS also stated that in August 2021, CRUSE paid for her, and other care coordinators, to travel to Las Vegas. THOMAS stated that Ms. Cruse paid for the hotel and flights. THOMAS stated that she had photographs of that trip on her phone.

28. Initially, THOMAS agreed to provide the videos to investigators, but at some point during the meeting, she decided she no longer wanted to speak to law enforcement and ended the interview without providing those videos.

29. Based on the interview with THOMAS's purported clients and THOMAS, it is clear that the billing records used to submit claims for payment to Medicaid by CTL were false.

30. The evidence on THOMAS's phone, particularly the video of CRUSE "doing billing" and teaching care coordinators how to fill out billing records is evidence of health care fraud in violation of 18 U.S.C. 1347.

31. Investigators from MECEAU reviewed information in the Medicaid Provider Database, kept by DHS in the regular course of its official business, and learned that CTL has had all reimbursement payments directly deposited into an account at US Bank since 03/19/2021. CTL received reimbursements from Wisconsin Medicaid totaling at least $1,063,022.22.

32. Case agents believe that monitoring of **TCP-1's** location will assist in identifying a place where the phone can be seized and searched, subject to legal process, for evidence of the crimes discussed herein.

TECHNICAL BACKGROUND

33. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

Cell-Site Data

34. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about **TCP-1**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically

determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

E-911 Phase II / GPS Location Data

35. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of **TCP-1**, including by initiating a signal to determine the location of **TCP-1** on the Service Provider's network or with such other reference points as may be reasonably available.

Pen-Trap Data

36. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communicationwithout revealing the communication's content. Currently, **TCP-1** has International Mobile Subscriber Identifier (IMEI) number 310240244294884 and Electronic Serial Number (ESN) 089235866509933378 .

Subscriber Information

37. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes

under investigation because the information can be used to identify **TCP-1**'s user or users and may assist in the identification of co-conspirators.

AUTHORIZATION REQUEST

38. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

39. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

40. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of **TCP-1** on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

41. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until March 1, 2023. This investigation is expected to remain covert at least until then, so disclosing the warrant would alert targets or subjects about the existence of a federal investigation. This investigation targets a sophisticated drug trafficking organization with multiple targets, subjects, and witnesses. Case agents will continue to request the same notification deadline for all warrants in this investigation, so that the notifications can be coordinated or extended as necessary. A single

notification date will reduce the administrative burden on case agents and the Court, minimize the risks of disclosure, and promote judicial economy. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of **TCP-1** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

42. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate **TCP-1** outside of daytime hours.

ATTACHMENT A

Property to Be Searched

1. Records and information associated with:

    - the cellular device assigned call number **(414) 779-3186** (referred to herein and in Attachment B as **"Target Cell Phone 1"** or "**TCP-1**"), that is in the custody or control of AT&T Mobility (referred to herein and in Attachment B as the "Service Provider" or "Provider"), a wireless communications service provider that is headquartered at 11760 U.S. Highway 1, Suite 600, North Palm Beach, FL 33408.

2. Target Cell Phone 1.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with **TCP-1** for the time period from February 1, 2021, to present:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

   vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);

   viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by **TCP-1**, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(B) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received).

b. Information associated with each communication to and from **TCP-1** for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which **TCP-1** or will connect at the beginning and end of each communication.

The Court has also issued an order(s) pursuant to 18 U.S.C. § 3123, dated today, for such information associated with **TCP-1**.

c. Information about the location of **TCP-1** for a period of **30 days**, during all times of day and night. "Information about the location of TCP-1" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of **TCP-1** on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), and 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) since February 2021.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this warrant.